Track: DNS

Comcast DNS

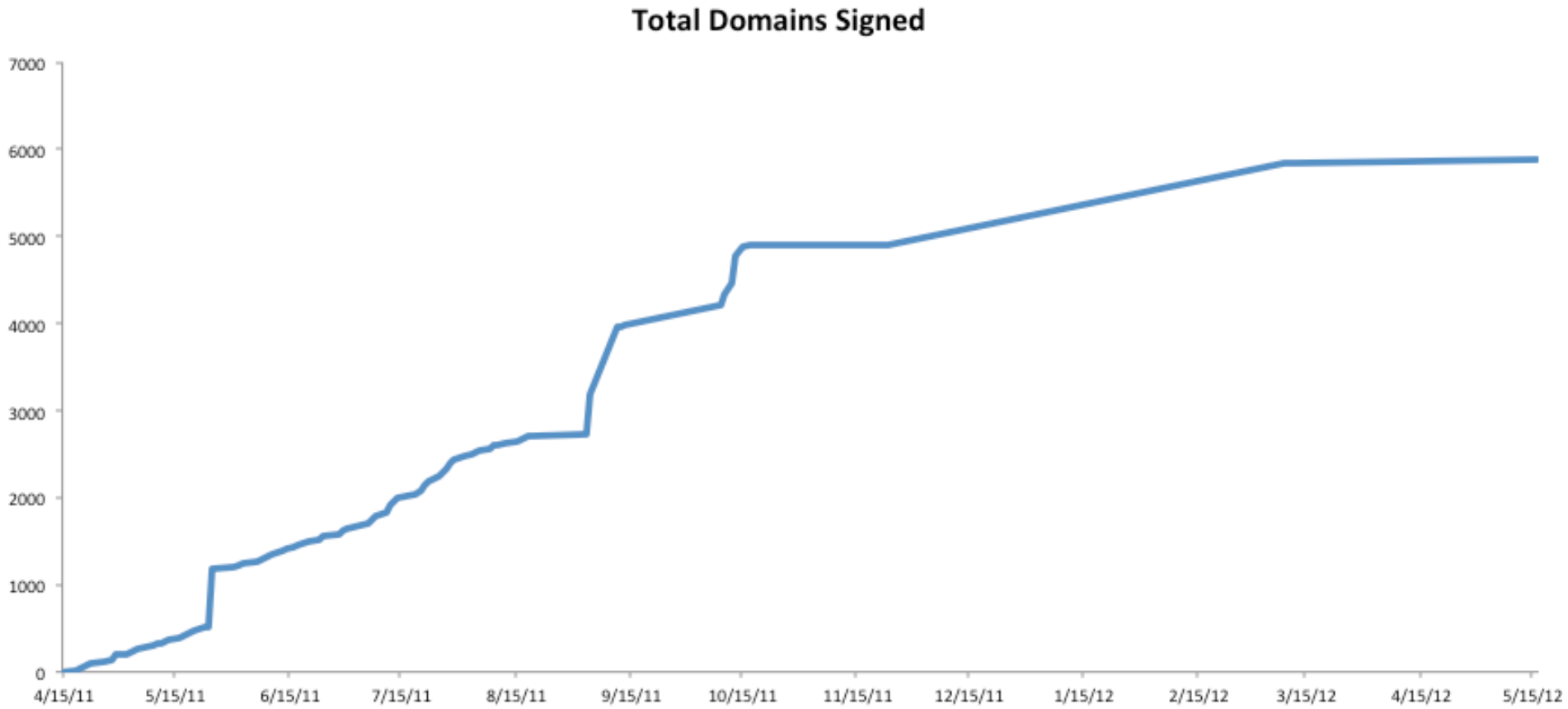
Tuesday, June 5, 2012

NATIONAL ENGINEERING & TECHNICAL OPERATIONS

DNSSEC – Update

We completed our DNSSEC deployment as of January 10, 2012.

- At the NANOG 54 DNS Track meeting, we discussed that we are now performing DNSSEC validation for all of our caching DNS traffic and had signed ~5,000 domains.
- We now have ~6,000 domains signed.



DNSSEC – Validation and Operational Issues

We have noticed the frequency of DNSSEC validation issues have been trending down over the past few months.

- There have been handful .GOV sites that experienced issues since NANOG 54.
  - One example consisted of the RRSIG record expiring, which caused the site to become unreachable for our customers.
  - Several social media channels contained complaints that Comcast was blocking services to this site.
  - After reaching out to the domain operator, it was corrected on 2 of 3 name servers of that domain.
  - After multiple attempts to contact the domain operator, a Negative Trust Anchor was required to restore services.
  - We have now removed this negative trust anchor.

DNSSEC – Current Operational Process

Our current process has evolved as the operational environment has changed.

- Social media channels have become a form of alerting for DNSSEC validation issues.
  - Twitter, Facebook, and blogs provide real time notification that a website is down.
- We leverage a variety of tools to identify and troubleshoot DNSSEC-related issues.
- A combination of data sources, such as WHOIS, SOA, and website contact information are used to initiate communication with domain operators which has yielded a ~50% success rate.
- Negative Trust Anchors are needed on occasion to provide domain operators time to correct their issues.
  - The use of Negative Trust Anchors is not meant to be a long term solution for domain operators or ISPs.

DNSSEC - Improving Time to Resolution

Goal: Reduce customer impact by improving operational efficiency and time to resolution.

- Some ideas we have for improving efficiency:
  - Tools like Google and Twitter Alerts, and paid aggregation applications are available to assist with social media, reducing the time to manually search for issues.
  - Applications or tools for identifying why a domain is not reachable due to a DNS failure, would reduce troubleshooting time and provide self-service tools for end users. Several good examples are:
    - http://dnsviz.net
    - http://dnssec-debugger.verisignlabs.com

DNSSEC – Evolution and Recap

DNSSEC operational practices are still maturing.

- Signing domains and completing key rollovers should be automated to minimize risk of failure.
- Like the creation of any new tool or process, it will improve as we learn and grow from our experiences.
  - This should result in moving all operational responsibility and accountability to the domain operators instead of ISPs.
  - It will reduce the need for troubleshooting and should eliminate the need for negative trust anchors.
- What are some other ideas for…
  - Improving the operational process for a failed domain?
  - Reducing the frequency of DNSSEC validation issues?
  - How customers know a domain is failing due to DNSSEC validation?

Thank You!

xfinity™

For more information on the Comcast DNSSEC and IPv6 deployments:

http://www.dnssec.comcast.net
http://www.comcast6.net
http://dns.comcast.net

Chris Ganster
chris_ganster@cable.comcast.com

Comcast
NATIONAL ENGINEERING & TECHNICAL OPERATIONS